Рекомендації щодо захисту персональних даних:

- для національних урядів,
- для донорських організацій
- для гуманітарних організацій
- для отримувачів гуманітарної допомоги
- для правозахисних організацій
- для медіа

Здійснено в рамках проекту за підтримки Фонду сприяння демократії Посольства США в Україні.
Погляди авторів не обов'язково збігаються з офіційною позицією уряду США.

Supported by the Democracy Commission Small Grants Program of the U.S. Embassy to Ukraine.
The views of the authors do not necessarily reflect the official position of the U.S. Government.

Freerights ASSOCIATION

EMBASSY OF THE UNITED STATES
KYIV, UKRAINE

Рекомендації щодо захисту персональних даних для національних урядів, для гуманітарних організацій:

- Розробити чітке національне законодавство, яке адекватно регулюватиме питання збору й обробки персональних даних, у тому числі в гуманітарних цілях (наприклад, передбачити застосовність Закону України «Про захист персональних даних» до діяльності, пов'язаної з наданням гуманітарної допомоги, у профільному законі).
- Оновити застаріле законодавство про захист персональних даних у разі, якщо воно не відповідає чинним міжнародним стандартам, не передбачає рамкових обмежень на використання автоматизованих технологій чи запобіжників від зловживань ними (як-от автоматизоване ухвалення рішень, системи, керовані штучним інтелектом тощо).
- Забезпечити можливість легкої та швидкої комунікації гуманітарних організацій з державними органами, відповідальними за захист даних, уможливити роз'яснення національних стандартів іноземним організаціям.
- Комунікувати з донорськими установами для послаблення вимог щодо передачі великих масивів персональних даних від гуманітарних організацій-реципієнтів як звітної інформації. Роз'яснювати чутливість контекстів, у яких оперують гуманітарні організації.
- Комунікувати злами державних баз даних і витоки даних, щоб гуманітарні організації мали уявлення про безпекову ситуацію з персональними даними в регіоні та безпосередньо в державах, де вони зареєстровані чи надають допомогу.

Рекомендації щодо захисту персональних даних для донорських організацій:

- Включити захист даних у планування проєктів і звітних форм, враховуючи чутливі контексти, у яких зазвичай оперують організації, що реалізують гуманітарні проєкти.
- Дотримуватися принципу мінімізації даних та утримуватися від вимагання надмірної кількості чутливої інформації (зокрема, не вимагати інформацію про стать, сексуальну орієнтацію, походження, належність отримувачів допомоги до маргіналізованих чи вразливих груп тощо).
- Бути гнучкими й адаптивними, коли безпосередній надавач допомоги зазначає про особливу чутливість отриманих даних і відмовляється включати таку інформацію до звітних форм.
- Переглянути технічні стандарти передачі даних від гуманітарної до донорської організації та посилити захист даних у разі, якщо виникають сумніви в надійності каналів комунікації. Якщо це неможливо, відмовитися від передачі особливо чутливих категорій даних.

Freerights ASSOCIATION

EMBASSY OF THE UNITED STATES KYIV, UKRAINE

Рекомендації щодо захисту персональних даних для гуманітарних організацій:

- Розробити політики захисту даних у випадках, якщо такі політики відсутні. Оновити застарілі чи нерелевантні політики, адаптувати їх до контексту роботи гуманітарної організації та технологій, які вона використовує при зборі й обробці даних.
- Розміщувати політики на видному місці на вебсайті організації, забезпечувати легкий доступ потенційних отримувачів допомоги до політик, вчасно повідомляти про їх оновлення.
- Зазначати в політиці, що вона застосовна до всіх видів обробки даних, які здійснює організація, або якщо політика застосована лише до збору даних через вебсайт, чітко згадувати про це в назві політики й давати посилання на політику, яка застосовна до інших зборів даних, зокрема процесів надання гуманітарної допомоги.
- Формулювати політики зрозумілою мовою, робити їх стислими й лаконічними (наприклад, Політика Світової продовольчої програми ООН на 130 сторінок явно не сприяє ознайомленню з нею пересічних отримувачів допомоги в критичних ситуаціях).
- Розробити версію політики, сформульовану доступною для дітей мовою, у разі, якщо фокусом організації є робота з дітьми та надання їм гуманітарної допомоги.
- Чітко і вичерпно описувати в політиці перелік даних, які збираються, і мету збору конкретних категорій даних (зокрема, це допоможе самим гуманітарним організаціям з'ясувати, чи вони не збирають дані в надмірних кількостях і чи є кількість даних пропорційною меті).
- Регулярно проводити оцінювання ризиків діяльності для захисту персональних даних, переглядати політики захисту даних залежно від контексту роботи, виду надаваної гуманітарної допомоги та засобів обробки даних, які використовуються організацією:
  - оцінювання має проводитися до, під час та після надання гуманітарної допомоги;
  - оцінювання має ґрунтуватися на рівні ризиків від певної активності, застосування певної технології чи певних дій у конкретному контексті;
  - оцінювання має орієнтуватися на підхід «приватність за замовчуванням»;
  - оцінювання має враховувати технологічний розвиток суспільства й ефективність технологій для подолання конкретних викликів;
  - оцінювання має мати прикладне, а не формальне значення.
- Уникати надміру широких підстав для збору і обробки даних при формулюванні політик захисту персональних даних, зокрема не включати «суспільний інтерес» чи «легітимний інтерес організації» до підстав обробки даних без належної деталізації.
- Мінімізувати збір даних, особливо у випадках, якщо організація є невеликою за кількістю персоналу й експертизою або нездатною повноцінно забезпечити безпеку даних з технічної та правової точки зору. Це особливо актуально тоді, коли організація планує збирати біометричні дані чи працює з технологіями, що потребують значного залучення технічних експертів.

Freerights ASSOCIATION

EMBASSY OF THE UNITED STATES KYIV, UKRAINE

- Надавати біженцям і шукачам притулку доступ до даних про них, пояснювати мету збору та порядок обробки даних, подальшу долю цієї інформації. У разі помилки в даних надавати можливість виправити інформацію.
- При використанні сторонніх ресурсів (програмного забезпечення, додатків чи вебсайтів, як-от «Trace the Face» у МКЧХ) для ідентифікації осіб, створення баз даних чи в інших цілях, пов'язаних з наданням гуманітарної допомоги, розміщувати політику захисту даних на таких ресурсах, викладати її зрозуміло й стисло, де можливо — додавати мови регіону, з яким гуманітарна організація активно працює.
- Утримуватися від поширення даних з державою чи іншими акторами, особливо коли це відбувається без попередження осіб, чиї дані планується передавати. У разі, якщо йдеться про вразливі групи, які можуть бути дискриміновані в державі, у якій надається гуманітарна допомога, дотримуватися максимальної конфіденційності в комунікаціях з державним сектором.
- Ретельно зважувати ризики при передачі систем прогнозування хвиль мігрантів, біженців та інших осіб, які потребують гуманітарної допомоги, державі (зокрема, як це сталося із системою, розробленою Danish Refugee Council). Це особливо важливо в контексті роботи в недемократичних режимах, де держава може спробувати обміняти дозвіл на роботу в регіоні на доступ до технологій.
- Призначити особу, відповідальну за захист даних, і розмістити контакти такої особи на вебсайті, щоб уможливити комунікацію будь-яких зацікавлених сторін з експертом із захисту даних усередині гуманітарної організації.
- Чітко вказувати підстави збору біометричних даних і те, наскільки це допомагає уникнути шахрайств, поліпшити процеси ідентифікації та знизити витрати на надання гуманітарної допомоги (включно з фінансовими й технічними розрахунками та показниками ефективності для доступних альтернатив збору персональних даних).
- Посилювати навички роботи з персональними даними в правовій і технічній площині для персоналу гуманітарної організації, який безпосередньо чи опосередковано працює з даними. Зокрема, у пригоді можуть стати освітні програми і сертифікації від МКЧХ та академічних закладів.
- Використовувати додатки з адміністрування паролів для посиленого захисту, що може убезпечити від використання викрадених персональних даних чи зламаних акаунтів для неправомірних активностей.
- Для уникнення витоків даних і зламів системи встановити програми застосування оновлень безпеки, регулярно проходити аудити для оцінювання вразливості систем (тестувати нові системи й перевіряти спроможність старих протистояти новим викликам і загрозам).
- Розробляти кризові протоколи на випадок зламів чи атак, які міститимуть чіткий алгоритм дій членів організації, залучених до роботи з персональними даними, регулярно переглядати та оновлювати такі протоколи залежно від контексту діяльності та застосовних технологій обробки даних.
- У випадку кібератаки чи витоку даних слід вчасно комунікувати з тими, чиї дані можуть опинитися чи опинилися під загрозою про наявну загрозу, проаналізувати прогалини в системі безпеки та оновити / посилити / змінити політики в разі потреби.
- Не використовувати для збору даних мережі на кшталт Telegram, Facebook чи інших незахищених соціальних мереж і месенджерів. Використовувати канали комунікації, які містять з'єднання peer-to-peer і можливість видаляти переписки із сервера для забезпечення максимальної конфіденційності.

Freerights ASSOCIATION
EMBASSY OF THE UNITED STATES KYIV, UKRAINE

Рекомендації щодо захисту персональних даних для отримувачів гуманітарної допомоги:

- Користуватися ініціативами захисту прав українців від правозахисних організацій, інформаційними ресурсами та керівництвами з отримання допомоги (на кшталт сторінки «Солідарність ЄС з Україною»).
- Обережно ставитися до надання персональних даних для отримання гуманітарної допомоги чи участі в так званих переписах населення на окупованих територіях, не розкривати інформації про військовослужбовців, членів їхніх сімей, громадських активістів, журналістів, культурних діячів.
- Уникати сайтів чи цифрових застосунків, у безпечності яких немає впевненості. Щонайменше не використовувати такі застосунки для передачі персональних даних.
- Уважно ставитися до електронних листів від незнайомих адресатів, повідомлень у месенджерах (Viber, Telegram, WhatsApp) з невідомих номерів телефону, а також повідомлень у соціальних мережах (Facebook, Instagram) від незнайомих користувачів, не відкривати підозрілі посилання та файли.
- За можливості при авторизації в інформаційних системах, сайтах, електронних кабінетах використовувати дво- або багатофакторну аутентифікацію та дотримуватися інших правил цифрової безпеки. З ними можна ознайомитися на ресурсі «Як?».
- Обережно ставитися до сканування QR-кодів для виконання будь-яких дій, пов'язаних з наданням персональних даних, отриманням допомоги чи інформації про надання допомоги, адже QR-код може вести до неперевірених посилань і, як наслідок, завантаження шкідливого програмного забезпечення й крадіжки даних з девайсу.
- Відмовитися від передачі персональних даних, включаючи паролі доступу до акаунтів, разові паролі, дані геолокації тощо, третім особам до моменту виникнення законних і необхідних підстав для збору такої інформації.
- Не надавати свої персональні дані та згоду на їхню обробку до моменту ознайомлення з метою та підставами обробки персональних даних, а також умовами їх обробки (зокрема, ознайомлення з політиками конфіденційності), крім випадків, коли відповідна обробка здійснюється на підставі закону для виконання володільцем даних покладених на нього обов'язків.
- Направляти запити щодо інформації про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження володільця чи розпорядника персональних даних.
- Висувати вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних, зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є неправильними.
- Відкликати згоду на обробку персональних даних (у випадку, якщо згоду було надано).
- Використовувати для отримання інформації надійні джерела, наприклад моніторинг IMI надає перелік добросовісних медіа, які дотримуються журналістських стандартів.
- Брати участь у розробленні політик захисту даних на рівні держави, гуманітарних і донорських організацій, ділитися досвідом щодо проблем, які виникли на практиці під час отримання гуманітарної допомоги, пропонувати рішення для посилення захисту даних, покращення політик конфіденційності тощо.

Freerights ASSOCIATION

EMBASSY OF THE UNITED STATES KYIV, UKRAINE

Рекомендації щодо захисту персональних даних для правозахисних організацій:

- Сприяти підвищенню рівня обізнаності гуманітарних організацій щодо правил роботи з персональними даними, оскільки не всі гуманітарні організації є правозахисними і тому можуть мати брак як правової, так і технічної експертизи.
- Ділитися позитивними практиками захисту даних (у тому числі формулюваннями політик), безпечного збору даних і їх передачі третім особам (за потреби), повідомляти про негативні досвіди для уникнення подібних ситуацій у роботі інших організацій.
- Засуджувати випадки порушення правил роботи з персональними даними, нехтувань технічною безпекою, зловживань чи маніпуляцій отримувачами допомоги завдяки більш привілейованому становищу гуманітарної організації (розпорядника ресурсів).
- Комунікувати проблемні випадки захисту даних і потенційні шляхи розв'язання проблем державі (регуляторні політики та звітування), донорським організаціям (звіти і обсяги даних), гуманітарним організаціям (потенційна зміна практики), громадянам (підвищення рівня цифрової грамотності, вміння захищати власні персональні дані).

Рекомендації щодо захисту персональних даних для медіа:

- Утримуватися від поширення неперевірених даних про порушення гуманітарними організаціями правил поводження з даними, оскільки неправдива інформація здатна підірвати довіру до гуманітарного сектору, спричиняючи неотримання допомоги тими, хто її потребує.
- Контактувати з організаціями, у яких, ймовірно, відбувся витік даних чи бази даних яких могли стати суб'єктом хакерської атаки, з метою верифікації інформації та отримання широкого погляду на проблему.
- Утримуватися від перебільшення наслідків витоків даних або кібератак (наприклад, DoS-атака не дорівнює зламу бази даних, відповідно шкода для персональних даних буде значно меншою, якщо не нульовою, тож їх не слід ототожнювати).
- У разі витоку даних у мережу утриматися від подальшого поширення персональних даних і збільшення аудиторії, яка має доступ до чутливої інформації.
- Популяризувати кампанії, спрямовані на підвищення обізнаності про правила захисту даних серед громадян і програми розвитку здатності гуманітарних організацій забезпечувати захист персональних даних (тренінги від держави, інших громадських організацій, академічної спільноти тощо).

Freerights ASSOCIATION

EMBASSY OF THE UNITED STATES KYIV, UKRAINE